UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/052,256	01/23/2002	Tomoru Teruuchi	13740-004001	1933

2292 7590 09/11/2006

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
NGUYEN, CHAU T	

ART UNIT	PAPER NUMBER
2176	

DATE MAILED: 09/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/052,256	TERUUCHI ET AL.	
	Examiner	Art Unit	
	Chau Nguyen	2176	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,7-10,13,17 and 19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-5, 7-10, 13, 17 and 19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/17/2006 has been entered. Claims 1, 3-5, 7-10, 13, 17 and 19 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-5, 7-10, 13, 17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer, European Patent Application No. 0586022 A1 in view of Serret-Avila et al. (Serret-Avila), US Patent No. 6,785,815, Serret-Avila (Serret-Avila2), US Patent Application Publication No. US 2005/0235154, and further in view of Karjoth et al. (Karjoth), US Patent Application Publication No. US 2001/0034839.

4. As to claims 1, 5 and 10, Fischer discloses an electronic signature method comprising the steps of:

analyzing a target document to generate a representation having a structure (page 20, lines 20-36: document package contains the cover letter 300, enclosed letter 302, spread sheet 304, graphics file 306);

generating electronic signatures corresponding to each structural element (page 20, lines 20-36: signature items A, C, E, and G represent the hash of the cover letter 300, enclosed letter 302, spread sheet 304, and graphics file 306, respectively); and

However, Fischer does not explicitly disclose generating a file signature code by encrypting said document as a whole and concatenating the generated file signature code and the electronic signatures from each of the said structural element into a single signature corresponding to the structure. Serret-Avila discloses a data signal 300 (a stream of textual information) is partitioned into a sequence of data blocks or segments 304, each segment 304 having its own signature 306 (Serret-Avila, col. 11, lines 23-45 and Fig. 3). In addition, Serret-Avila discloses each data block or segment is hashed (assigned a unique key), and all the unique keys from each data block are concatenated, resulting the signature 810 (a file signature code) which is encrypted (col. 18, lines 12-34). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Serret-Avila and Fischer to include generating a file signature code by encrypting said document as a whole and

concatenating the generated file signature code and the electronic signatures from each of the said structural element into a single signature corresponding to the structure. Serret-Avila suggests that the hash values (all unique keys) in hash concatenation are used to verify the authenticity of the corresponding blocks in the data signal, and also to control access to and use of digital/electronic data.

However, Fischer and Serret-Avila do not explicitly disclose the target document stored in a format representing a tree structure to generate the tree structure of the target document structure in a memory. Serret-Avila2 discloses a memory unit for storing a digital signature and a plurality of hash values related to the data file, the digital signature and the plurality of hash values forming a hierarchy or tree (page 3, paragraph [0019]). Since Serret-Avila2 discloses a system and method for authenticating an protecting the integrity of data streams and other data, which is similar to protecting data using digital signature of Fischer and Serret-Avila, thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Serret-Avila2 and Fischer and Serret-Avila to include the target document stored in a format representing a tree structure to generate the tree structure of the target document structure in a memory. Serret-Avila2 suggests that the hierarchy culminates with a signed hash that can be sued to verify the integrity of other hash values in the hierarchy, and the other hash values can be used to efficiently verify the authenticity of arbitrary portions of the content file.

Fischer, Serret-Avila and Serret-Avila2 disclose the step of a level of tree structure at which said electronic signatures are to be generated, whereby a level of limitation of a document to be electronically signed can be varied (Serret-Avila2, page 2, paragraph [0017] and page 8, paragraphs [0091]-[0092]). However, Fischer, Serret-Avila and Serret-Avila2 do not explicitly disclose setting a depth code designating a level of the tree structure said electronic signature is to be generated. Karjoth discloses computing the hash component of the tree beginning at depth d and proceeding the root at depth 0 such as forming the hashes for the leaves at level d, and then the hash values at level d-1 and so on towards to root, and then the application provider AP signs the hash tree at the root node and assigns its signature (pages 4-5, paragraphs [0060]-[0064]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Karjoth and Fischer, Serret-Avila and Serre-Avila2 to include setting a depth code designating a level of the tree structure in order to calculate the hash value of the tree at the root and assign a signature to the hash value of the tree.

5. As to claims 3, 9 and 19, Fischer, Serret-Avila and Serret-Avila2 disclose wherein a rate of coincidence between the target document and the target document with an electronic signature is found from a rate of structural elements having authenticated electronic signatures to the whole structure (Fischer, page 20, lines 20-36).

6. As to claims 4, 7 and 13, Fischer, Serret-Avila and Serret-Avila2 disclose wherein said concatenating step includes putting the generated file signature code and the generated electronic signatures in a row (Serret-Avila discloses a data signal 300 (a stream of textual information) is partitioned into a sequence of data blocks or segments 304, each segment 304 having its own signature 306 (Serret-Avila, col. 11, lines 23-45 and Fig. 3). In addition, Serret-Avila discloses each data block or segment is hashed (assigned a unique key), and all the unique keys from each data block are concatenated as shown in a row of H(B1), H(B2), H(B3),... H(Bn), resulting the signature 810 (col. 18, lines 12-34). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Serret-Avila and Fischer to include concatenating the generated electronic signatures in a row into a single signature corresponding to the structure of the generated representation. Serret-Avila suggests that the hash values (all unique keys) in hash concatenation are used to verify the authenticity of the corresponding blocks in the data signal, and also to control access to and use of digital/electronic data).

7. As to claims 8 and 17, Fischer, Serret-Avila and Serret-Avila2 disclose means for analyzing the structure of the target document to verify the target document having the generated electronic signature (Fischer, page 20, lines 20-36); and

means for analyzing each of the electronic signatures of the structural elements of the target document (Fischer, page 20, lines 20-36).

Response to Arguments

8. In the remarks, Applicant(s) argued in substance that

A) None of the prior art teaches or suggests the feature of setting a depth code designating a level of the tree structure at which the electronic signatures are to be generated whereby a level of limitation of the document to be electronically signed can be varied as recited in claims 1, 5 and 10.

In reply to argument A, Fischer, Serret-Avila and Serret-Avila2 disclose the step of a level of tree structure at which said electronic signatures are to be generated, whereby a level of limitation of a document to be electronically signed can be varied (Serret-Avila2, page 2, paragraph [0017]: multi-level hierarchy of hash values is generated from the digital file (document), and root hash value is digitally signed and being derived from each of the hash values in the hierarchy, and the tree structure of the hierarchy is scalable (varied) (and page 8, paragraphs [0091]-[0092])). However, Fischer, Serret-Avila and Serret-Avila2 do not explicitly disclose setting a depth code designating a level of the tree structure said electronic signature is to be generated. Karjoth discloses computing the hash component of the tree beginning at depth d and proceeding the root at depth 0 such as forming the hashes for the leaves at level d, and then the hash values at level d-1 and so on towards to root, and then the application provider AP signs the hash tree at the root node and assigns its signature (pages 4-5,

paragraphs [0060]-[0064]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Karjoth and Fischer, Serret-Avila and Serre-Avila2 to include setting a depth code designating a level of the tree structure in order to calculate the hash value of the tree at the root and assign a signature to the hash value of the tree.

B) Karjoth clearly indicates that hash values for the entirely of the code blocks are calculated, and thus contrary to the feature of setting a depth code designating a level of the tree structure at which the electronic signatures are to be generated.

In reply to argument B, Karjoth discloses on page 4, paragraphs [0060]-[[0064] that the tree has depth d, where the root is at depth 0, and there are 2 to the i nodes at level I, the tree T has exactly n leaves associated with the values of A1, A2,,..., An such as T with n=2 to the d(depth) . Then beginning at depth d and proceeding to the root at depth 0, each node j is labeled with Hj (hash value), and the label at the root denoted H(T) is a hash value that depends on A1, A2,..., An (nodes).

9. Applicant's arguments filed 07/17/2006 have been fully considered but they are not persuasive. Please see the rejection and response to arguments above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chau Nguyen whose telephone number is (571) 272-4092. The Examiner can normally be reached on Monday-Friday from 8:30 am to 5:30 pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Heather Herndon, can be reached at (571) 272-4136.

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. On July 15, 2005, the Central Facsimile (FAX) Number will change from 703-872-9306 to 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chau Nguyen
Patent Examiner
Art Unit 2176

William L. Bashore
WILLIAM BASHORE
PRIMARY EXAMINER